分布式共识

2022年2月17日 9:34

What.

多个节点的可独自操作或记录的情况下.

使得所有节点针对某个状态达成一致的过程.

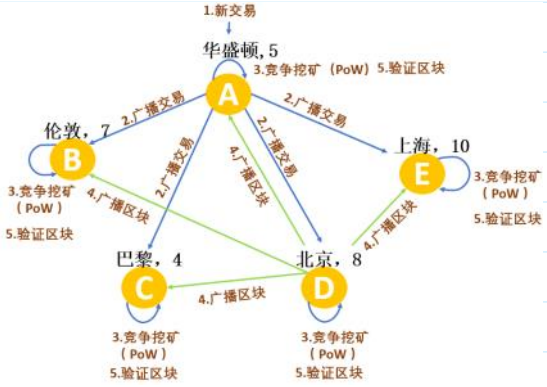
挖矿

所有 server 帮助记录交易并达成一致的过程.

分布式共识方法.

关键点 { 获取记账权. 有且仅有一个 node 有记账权.
所有结点达成一致. 其他 node 同意该节点的记账结果 }

① PoW (Proof-of-work) 工作量证明.



- 客户端 A 产生新的交易，向全网进行广播，要求对交易进行记账。
- 每个记账节点接收到这个请求后，将收到的交易信息放入一个区块中。
- 每个节点通过 PoW 算法，计算本节点的区块的哈希值，尝试找到一个具有足够工作量难度的工作量证明。
- 若节点 D 找到了一个工作量证明向全网广播。当然，当且仅当包含在该区块中的交易都是有效且之前未存在过的，其他节点才会认同该区块的有效性。
- 其他节点接收到广播信息后，若该区块有效，接受该区块，并跟随在该区块的末尾，制造新区块延长该链条，将被接受的区块的随机哈希值视为新区块的随机哈希值。

② PoS (Proof-of-Stake) 权益证明.

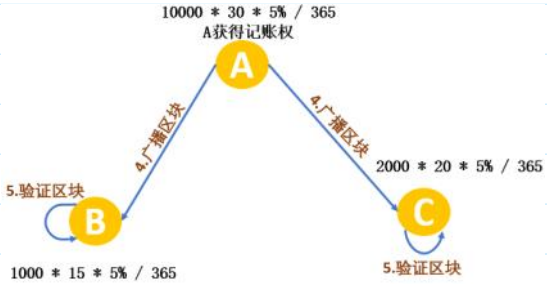
核心：由系统权益代替算力. → 由此鼓励"利滚利".

↘每个 node 占有的货币数量和时间.

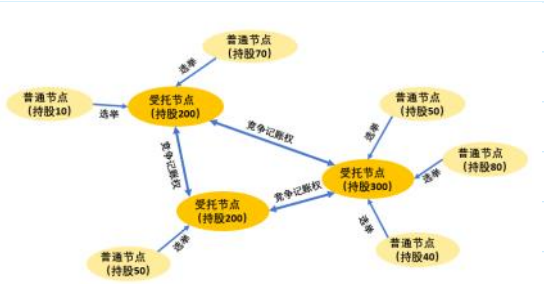
↘节点获得的奖励.

在股权证明 PoS 模式下，根据你持有货币的数量和时间，给你发利息。每个币每天产生 1 币龄，比如你持有 100 个币，总共持有了 50 天，那么，你的币龄就为 5000。这个时候，如果你发现了一个 PoS 区块，你的币龄就会被减少 365。每被减少 365 币龄，你就可以从区块中获得 0.05 个币的利息 (可理解为年利率 5%)。

在这个案例中，利息 = （5000*5%）/365 = 0.68 个币。这下就有意思了，持币有利息。



③ DPoS (Delegated Poof of Stake) 委托权益证明.



	PoW	PoS	DPoS
计算消耗	高	中	低
结构类型	去中心化	去中心化	去中心化（多中心）
交易量/秒	PoW < PoS < DPoS		
交易服务费	高	低	低
应用区块链平台	比特币	以太坊	比特股

一致性和共识.

- 一致性：主从数据的对外一致性. 重点：最终对外表现的结果.

共识：系统中所有进程对该修改意见达成一致. 重点：达成一致的过程.